Elektronische Zustellung Modell und Prozesse			Konvention zusemod-1.4.0 Ergebnis der AG
Kurzbeschreibung	Die elektronische Zustellung ist ein zentraler Bestandteil des E-Government Frameworks. Dieses Papier beschreibt Grundlagen und Prozessmodell der elektronischen Zustellung. Dabei wird ein modularer, universeller, ökonomischer Zustelldienst vorgeschlagen, der die einzelnen Fachapplikationen von den Details der Zustellung entlastet.		
Autor(en):	Peter Reichstädter Arne Tauber	Projektteam / Arbeitsgruppe: AG-ZUSE / AG-II	
Beiträge von:	Thomas Rössler, Arno Hollosi, Bernhard Karning, Christian Herwig, Gerhard Schwarz, Vinzenz Wukits uva.		

Version 1.4.0 : **02.02.2012**	Fristablauf: **TT.MM.JJJJ**
Abgelehnt von:	*(Länderangabe bei ablehnender Stellungnahme)*

Unter-Version ... : **TT.MM.JJJJ**	Fristablauf: **TT.MM.JJJJ**
Abgelehnt von:	*(Länderangabe bei ablehnender Stellungnahme)*

Detail-Version ... : **TT.MM.JJJJ**	Fristablauf: **TT.MM.JJJJ**
Anmerkungen:	*(Detailangaben zur Freigabe)*

Inhaltsverzeichnis

1 Motivation und Grundlagen

Für die öffentliche Verwaltung ist die Zustellung von Schriftstücken eine zentrale aber auch ressourcenintensive Schnittstelle zu ihren Empfängern[1]. Die elektronische Zustellung ist nicht zuletzt aus diesem Grund ein wesentlicher Bestandteil einer zukunftsweisenden elektronischen Verwaltung. Dabei werden hohe, teils widersprüchliche Anforderungen an diese Art der Zustellung gestellt. Das im Folgenden beschriebene Modell bietet einerseits einen größtmöglichen Komfort auf Seiten der Empfänger (BürgerInnen), andererseits wesentliche Vereinfachungen, Synergien, und Einsparungspotentiale auf Seiten der öffentlichen Verwaltung.

1.1 Gesetzliche Voraussetzungen

Die Zustellung erfordert eine qualitativ hochwertige Identifizierung und Authentifizierung der Empfänger. Mit dem Konzept Bürgerkarte und der damit geschaffenen Basis für elektronische Signaturen kann der elektronische Prozess diesen Anforderungen gerecht werden. Einerseits kann durch Einsatz von qualifizierten elektronischen Signaturen laut Signaturgesetz [SIGG07] [SIGV07] der elektronische Prozess diesen Anforderungen gerecht werden. Andererseits bildet das E-Government-Gesetz [EGOVG07] die rechtliche Basis für die Bürgerkarte, die auf einem qualifizierten Zertifikat beruht, und somit eine qualifizierte elektronische Signatur enthält, die ebenfalls eine ausreichende Qualität für die Abwicklung der Zustellung besitzt. Die Identifikation, die im Rahmen der Registrierung der Signaturzertifikate und der Aufbringung der Personenbindung zwingend durchgeführt werden muss, kann im Zustellverfahren unmittelbar weiter verwendet werden, da sich die Identität einer Person nicht ändert.

Unabdingbar für eine erfolgreiche Zustellung ist das Bescheinigen des Empfangs des Schriftstücks seitens des Empfängers in Form eines Zustellnachweises (§ 35 Abs. 3 [ZUSTG]). Auch hier kann die bürgerkartenkonforme elektronische Signatur eingesetzt werden, da sie die notwendige rechtliche Wirkung entfaltet.

Im Sinne des E-Government werden Schriftstücke, die nachweislich übermittelt werden sollen, nicht direkt zugestellt (z.B. per E-Mail), sondern es wird eine Hinterlegung an der Zustelladresse „an der sich die Person aufhält“ durchgeführt (Zustelladresse kann sein Abgabestelle bzw. elektronische Zustelladresse - vgl. auch § 2 Z 3 [ZUSTG]). Dies ist notwendig, da E-Mail keine ausreichende Garantie und Kontrolle darüber bietet, ob und wann ein Schriftstück beim Empfänger angelangt ist. Im E-Government ist die „Abgabestelle“ ein Server im Internet (der Zustelldienst), welcher den Empfänger[2] von der Hinterlegung auf geeignete Weise informiert.

1.2 Anforderung an die Zustellung

Aus der Sicht des Datenschutzes, der Sicherheit und der organisatorischen Rahmenbedingungen müssen eine Reihe von Anforderungen erfüllt werden:

---

[1] Zum Beispiel versenden das Finanz- und Justizministerium gemeinsam jährlich über 30 Millionen Schriftstücke.

[2] Die in diesem Beitrag verwendeten Personenbegriffe wie z.B. „Empfänger“ beziehen sich gleichermaßen auf weibliche und männliche Personen bzw. steht Empfänger für Kunde, Bürger, … .

- Die Übertragung über offene Netzwerke (Internet) hat generell verschlüsselt stattzufinden. Zudem sollen Dokumente an den Zustelldienst bereits in auf den Empfänger bezogener verschlüsselter Form angeliefert werden können.
- Die zuzustellenden Schriftstücke sollen seitens der ausgebenden Behörde signiert sein – „Amtssignatur“ (vgl. auch § 19 [EGOVG07] bzw. § 18 Abs. 4 [AVG07]). Damit wird die Authentizität des Schriftstücks für die Empfänger verifizierbar.
- Es muss äquivalent zur herkömmlichen Zustellung authentische Zustellnachweise im Falle einer vollzogenen Zustellung und Unzustellbarkeitsanzeigen im Falle der Unzustellbarkeit geben. Beide Strukturen müssen geeignet strukturierte Meta-Informationen über das zugestellte Schriftstück enthalten, sodass eine automatisierte Verarbeitung und Zuordnung zum ursprünglichen Geschäftsfall beim Absender möglich ist.
- Die notwendige Infrastruktur zum Erstellen und Prüfen von Signaturen muss auf Seiten der Empfänger und Behörden vorhanden sein. Auf Empfängerseite wird diese Anforderung mit dem österreichischen Konzept Bürgerkarte POWB02] abgedeckt, auf Behördenseite mit den generischen Server-Signaturkomponenten [MOA].

1.3 Bausteine

Der Zustellprozess bedient sich verschiedener Bausteine:

- Eines zentralen Zustellkopfes (siehe auch [ZUSEKOPF]), welcher die Anfragen der zustellenden Institutionen hinsichtlich Auswahl des möglichen Zustelldienstes entgegennimmt und entsprechende (positive oder negative) Antworten retourniert.
- Eines Zustelldienstes, welcher der Absenderapplikation die zuzustellende Sendung abnimmt und dies gegenüber der Applikation und dem Empfänger verbindlich protokolliert. Weitere serviceorientierte Dienste, wie beispielsweise ein Dokumentensafe, Ausdruckmöglichkeit, etc. können vom Zustelldienst angeboten werden, sind aber nicht Teil dieser Spezifikation.
- Eines Systems der Verständigung, das den Empfänger von der Hinterlegung des Schriftstückes informiert. Diese Verständigung kann auf unterschiedliche Weise erfolgen (E-Mail, SMS, etc. bzw. auch postalisch (vgl. [ZUSTG] § 35 Abs. 2]).
- Der eigentlichen Abholung beim Zustelldienst.
- Einem Nachweis der erfolgten Zustellung bzw. Unzustellbarkeit für die spätere Nachforschung.

1.4 Generelle Begriffsbestimmungen

Im Folgenden Abschnitt werden die in der Spezifikation verwendeten Begriffe zusammengefasst und allgemeingültig erklärt bzw. mit Beispielen unterlegt; sollten Begriffe nicht eindeutig beschrieben werden, zählt letztendlich die Definition, wie Sie im ZustG07 festgelegt wurde.

Zustellstück: ist ein elektronischer (evt. verschlüsselter) Datencontainer. In diesem Datencontainer wird sich in der Regel eine durch den Versender signierte Datei, etwa ein Bescheid, befinden. Sofern keine Verschlüsselung stattfindet, kann aus Datenschutzgründen nur ein verschwiegenheitsverpflichteter Dienstleister den Zustelldienst betreiben. Bestimmte Zustellstücke dürfen implizit nur verschlüsselt elektronisch zugestellt werden (Medizinische Daten, sensible Daten, Personenbezogene Daten, etc. - siehe auch § 14 Datenschutzgesetz bzw. im speziellen jeweiliges Materiengesetz (z.B.GesundheitstelematikGesetz, etc.); sollte

allerdings für zuvor genannte Zustellstücke die Verschlüsselung nicht möglich sein, MUSS konventionell zugestellt werden.

Zustellregistrierung: darunter versteht man die Registrierung von Empfängern bei einem elektronischen Zustelldienst; sie registrieren sich zu diesem Zweck beim Zustelldienst mit persönlichen Daten (Name, Geburtsdatum,etc.) sowie Verständigungsadressen (elektronisch und (optional) postalisch) und „zulässigen" Dokumentenformaten (z.B. .doc, .pdf, .xls, .html, etc). Der Zustelldienst MUSS jedenfalls jene Dokumentenformate (MIME-Types) verarbeiten und zustellen können, welche durch die E-Government Kooperation als geeignete Dokumentformate für die Kommunikation in Richtung Bürger empfohlen worden sind (siehe [DOKFORM] Abschnitt (2)). Der Zustelldienst MUSS dem Bürger (Empfänger) im Zuge der Erstregistrierung diese Dokumentenformate zur Annahme empfehlen.). Im Zuge der Registrierung können Empfänger auch gleich ihre persönlichen Schlüssel zur Verschlüsselung der Schriftstücke bekannt geben bzw. werden auch mögliche Abwesenheiten an dieser Stelle administriert.

Zustelldienst/-service: Dieser besitzt für seine registrierten, potentiellen Empfänger die Zustell- und Verständigungsadressen. Eine Identifikation der Empfänger kann einerseits über ein bereichsspezifisches Personenkennzeichen (bPK) erfolgen (die Zustellung dient dabei als eigenes Verfahren zur Bildung der bPK via des in Abschnitt 3.2.2. beschriebenen Stammzahlenregisters). Andererseits kann die Zuordnung auch über Namen und Geburtsdatum bzw. Namen Verständigungsadressen erfolgen (Angaben erfolgen jeweils bei der Registrierung).

Verständigung: Eine zwischen Zustelldienst und Empfänger vereinbarte automatische Benachrichtigung über die Hinterlegung einer Sendung. Diese wird in den meisten Fällen nicht die für die Zustellung selbst notwendigen Sicherheitsmerkmale aufweisen (Sicherheit des Einlangens bzw. Vertraulichkeit). Die Verständigung kann etwa über SMS, E-Mail, oder andere Medien erfolgen. Die Verständigung ist hinsichtlich ihrer Metadaten (Rang, Zeitpunkt, Art, …) zu protokollieren. Eine elektronische Zustellung mit Nachweis kann, falls es nach den beiden elektronischen Verständigungen zu keiner Abholung gekommen ist und der Empfänger eine postalische Adresse angegeben hat, eine konventionelle Verständigung (‚Postkarte') bedingen (§ 34 Abs. 2 [ZUSTG]).

Datenschließfach des Empfängers: Datenbereich, der in technisch gesicherter Weise nur dem Empfänger zugänglich ist. Wird eine hinreichend hochwertige Verschlüsselung und damit verbundenes Schlüsselmanagement verwendet, könnte dies in Zukunft auch als Ablagefach (Datensafe) für andere elektronische Dokumente des Benutzers herangezogen werden.

Zustellung: Abholung der/des eingelangten Zustellstücke(s)

Zustellnachweis: sofern vom Sender gefordert, werden die relevanten Metainformationen (Zeitpunkt der Zustellung, Identifikationsmerkmale, …) mittels eines Zustellnachweises rückübermittelt. Im Falle einer Unzustellbarkeit, d.h. die Zustellung wird elektronisch nie bezogen, wird dem Sender ebenfalls eine so genannte „Unzustellbarkeitsanzeige" übermittelt, um ggf. auf Seite des Versenders reagieren zu können.

2 Der Zustellprozess

2.1 Abkürzungen

Folgende Abkürzungen werden in diesem Dokument verwendet:

Tabelle 1 - Abkürzungen

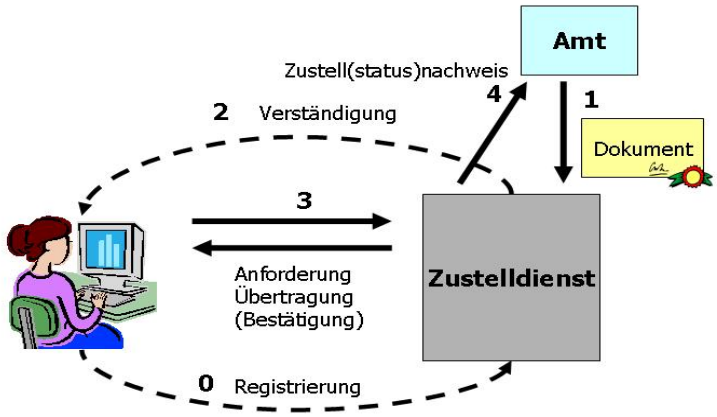
Abkürzung	Erläuterung
SZ	Stammzahl des Empfängers
SZR	Stammzahlenregister
ZbPK	Bereichsspezifisches Personenkennzeichen des Empfängers (für den Bereich Zustellung = urn:publicid:gv.at:cdid+ZU)
vZbPK	verschlüsseltes bereichsspezifisches Personenkennzeichen des Empfängers (für den Bereich Zustellung = urn:publicid:gv.at:ecdid+ZU) bezogen auf den Zustelldienst
VN	Vorname des Empfängers
NN	Nachname des Empfängers
ADR	Adresse des Empfängers – ZMR-Konformität kann vom Zustelldienst geprüft werden
GEBDAT	Geburtsdatum des Empfängers

2.2 Allgemeine Prozessbeschreibung

Das Modell geht davon aus, dass die Senderapplikation das Schriftstück an einen passenden Zustelldienst übergibt und danach weder das Dokument noch Metainformationen über das Dokument evident halten muss (Anm.: Statusinformationen über die erfolgte Zustellung des Dokumentes können, falls erforderlich, rückübermittelt werden). Weiters geht das Modell davon aus, dass die Person dem Zustelldienst bereits bekannt ist. Das heißt, die Person registriert sich beim Zustelldienst und gibt dort die notwendigen Daten, die für eine Identifizierung notwendig sind, bekannt. Im Besonderen werden dabei die Schlüssel zur Dokumentverschlüsselung bekannt gegeben. Da Personen der elektronischen Zustellung explizit zustimmen müssen, kann der Registrierungsprozess auch gleich diese Zustimmung einholen (siehe auch Abschnitt 2.3. ff für detaillierte Informationen).

Die folgende Figur zeigt den Ablauf in exemplarischer Form:

Abbildung 1 – Einzelne Schritte des Zustellprozesses



0. Bei der Anmeldung (Registrierung) zur elektronischen Zustellung muss sich der Benutzer mit der Bürgerkarte bei einem elektronischen Zustelldienst identifizieren. Benutzer können sich bei einem oder mehreren Zustelldiensten zur elektronischen Zustellung registrieren.

1. Das Schriftstück wird durch die Senderapplikation (z.B. im Bild das Amt) in einer für den Empfänger bestimmten (verschlüsselten) Form sowie mit den notwendigen Anforderungen (Rückschein, Geschäftszahl, etc.) angeliefert. Ein etwaiger Verschlüsselungsschlüssel wird im Rahmen des Schnittstellen-Protokolls vom Zustelldienst an die Applikation übergeben (siehe Abschnitt 2.3 dieses Dokumentes bzw. Abschnitt: Abfrage beim zentralen Zustellkopf [ZUSEKOPF]).

2. Es erfolgt eine elektronische Verständigung in der durch den Empfänger gewünschten Form. Wird das Schriftstück darauf hin nicht abgeholt, erfolgt eine zweite elektronische Verständigung. Sofern das Schriftstück darauf hin noch immer nicht abgeholt wird, erfolgt - sofern eine postalische Abgabestelle am Zustelldienst hinterlegt ist - eine dritte postalische Verständigung.[3] Am ersten Werktag nach der zweiten elektronischen Verständigung bzw. am dritten Werktag nach der dritten postalischen Verständigung beginnt der Fristenlauf (zum Beispiel Einspruchsfristen), wenn das Schriftstück nicht abgeholt wird. Dies deshalb, da der Empfänger Kenntnis über das Vorhandensein des Schriftstücks hat und es jederzeit abholen kann. Das Verfahren wartet also nicht, bis er das (möglicherweise „unangenehme“) Schriftstück abholt.

3. Der Empfänger holt sein Zustellstück ab. Dabei stellt der Zustelldienst, sofern vom Sender gefordert, implizit mittels einer Benutzerinteraktion einen elektronischen (und signierten) Zustellnachweis pro Zustellstück aus; damit wird vermieden, dass der Empfänger pro Zustellstück eine signierte Zustellbestätigung abgeben muss. Danach kann er das verschlüsselte Dokument in Empfang nehmen und lokal bei sich entschlüsseln – Hinweise dazu siehe [ZUSEMSG]. Der Zustellnachweis wird sowohl vom Zustelldienst evident gehalten, als auch der Behörde unmittelbar übermittelt. § 35 Abs. 3 [ZUSTG] ermöglicht auch eine Identifikation und Authentifizierung durch eine an die Verwendung sicherer Technik gebundene automatisiert ausgelöste elektronische

[3] Bei Zweifeln, ob oder wann eine elektronische Verständigung beim Empfänger eingelangt oder eine Verständigung zugestellt worden ist, hat die Behörde die Tatsache und den Zeitpunkt des Einlangens bzw. der Zustellung von Amts wegen festzustellen [ZustG07].

Signatur. Diese Art der Abholung entspricht einer Abholung auf Basis einer besonderen Vereinbarung (gem. §35(3) [ZUSTG]) und erfordert die Abholung von Zustellstücken unter Verwendung eines (SSL-)Client-Zertifikates, wodurch im täglichen Umgang mit der Zustellung jede weitere Interaktion mit dem Zustelldienst unter Verwendung der Bürgerkarte entfällt. Der Zustellnachweis erfolgt dabei mit der „Technologie der Signatur" beim Zugang mit Clientzertifikat (SSL) implizit (im Zuge des SSL-Handshakes). Dieser Vorgang wird vom Zustelldienst protokolliert (Zeitpunkt, Zertifikat, Gültigkeit); als Annahmezeitpunkt der Zustellung gilt der protokollierte Zeitpunkt der Authentifikation (SSL-Handshake). Langen während einer zertifikatsaktivierten E-Mail-Client-Session (IMAP) weitere Zustellstücke ein, so werden diese erst nach erneutem SSL-Verbindungsaufbau (erneutem Handshake) und damit Zustellnachweis als E-Mail übermittelt – Details dazu siehe [ZUSEMAIL].

4. Sollte die Zustellung (bzw. Hinterlegung) fehlschlagen, leitet der Zustelldienst eine Rückzustellung in Form einer „Unzustellbarkeitsanzeige" der relevanten Meta-Informationen betreffend des gescheiterten Zustellversuchs an den Sender des Schriftstücks (das Amt) ein. Die eigentlichen Nutzdaten der Zustellung (aus der Applikation kommend) müssen am Zustelldienst vernichtet werden.

Der Empfänger kann beim Zustelldienst jederzeit seine „elektronische Abwesenheit" bekannt geben, um damit die Zustellmöglichkeit temporär zu unterbinden (dabei bedeutet eine Abwesenheitsmeldung von z.B. 6. - 20. Mai dass bis zum 5. Mai 23:59:59 bzw. wieder ab 21. Mai 00:00:00 zugestellt wird (d.h. Tag-genau bzw. Datum der Abwesenheit ist immer inklusive zu verstehen).

Das beschriebene Modell stellt sicher, dass der Zustelldienst oder Dritte zu keinem Zeitpunkt Einsicht in das Schriftstück nehmen können. Dadurch ergibt sich die Möglichkeit, ohne weitere Bedenken den Zustelldienst auch von externen Dienstleistern betreiben zu lassen, da sie keine Einsicht nehmen können, aber dennoch die Zustellung ordnungsgemäß vollziehen können.

2.3 Prozesse im Detail

2.3.3 Prozess: Registrierung von Empfängern

Dieser Prozess behandelt die für die erstmalige Registrierung von Empfängern und die damit notwendige Erfassung von empfängerrelevanten Daten sowie die für die Registrierung notwendige qualitätsvolle Identifikation.

2.3.3.1 Qualitätsvolle Identifikation

Wesentlich für die elektronische Zustellung ist die qualitätsvolle Identifikation der Empfänger. Diese Identifikation muss zum einen bei der Registrierung des Empfängers verwendet werden, damit eine eindeutige Zuordnung der empfängerrelevanten Daten zum Empfänger erfolgen kann. Zum anderen stellen die gesetzlichen Rahmenbedingungen der Zustellung bei bestimmten Zustellqualitäten (bisherige Formen: RSa, RSb) sehr hohe Ansprüche an die Identifikation des Empfängers, welche in Folge bei der Abholung eines Zustellstücks maßgeblich ist.

Eine technische Lösung für die qualitätsvolle Identifikation bietet die Identifikation mittels der Personenbindung [HOLL02] bzw. [HOKP01] und der Signaturfunktion einer Bürgerkarte (qualifizierte Signatur). Dieses Prinzip wird in MOA-ID beschrieben [MOA]. Zudem ermöglicht § 35 Abs. 3 ZustG07 auch eine Identifikation und Authentifizierung durch eine an die Verwendung sicherer Technik gebundene automatisiert ausgelöste elektronische

Signatur (dies bedarf allerdings einer besonderen Vereinbarung zwischen Empfänger und Zustelldienst) – Dieses Prinzip wird in [ZUSEMAIL] beschrieben. Letzere Art der Authentifizierung kann ausschließlich für die Abholung genutzt werden. Die Registrierung eines elektronischen Postfachs bedingt in jedem Fall die Verwendung der Bürgerkarte.

2.3.3.2 Natürliche Personen

Die Registrierung von natürlichen Personen erfolgt in folgenden Schritten:

2.3.3.3 Schritt 1: Qualitätsvolle Identifikation

Eine qualitätsvolle Identifikation wird durchgeführt. Die vom SZR signierten Daten der Personenbindung (VN, NN, GEBDAT, SZ) des Empfängers werden ausgelesen. Aus der Stammzahl wird die Zustell-bPK errechnet und abgelegt. Der Empfänger signiert die Anmeldedaten und beweist damit gegenüber dem Zustelldienst seine Identität.

2.3.3.4 Schritt 2: Optionale Ergänzung der zugehörigen Adressdaten

Nach Schritt 1 können die zugehörigen Adressdaten ergänzt werden. Mit den im vorigen Schritt aus der Personenbindung gewonnenen Daten kann eine optionale Anfrage an das zentrale Melderegister durchgeführt werden, um die Adressdaten (für eine eventuelle optionale postalische Verständigung) des Empfängers zu validieren.

2.3.3.5 Schritt 3: Angabe der Verständigungsadressen

Der Empfänger muss zumindest eine elektronische Verständigungsadresse angeben, wobei die Verfügungsberechtigung zur elektronischen Verständigungsadresse vom Zustelldienst geprüft werden muss (z.B. durch die Übermittlung eines E-Mail Aktivierungslinks bzw. eines zufälligen Begriffs an die jeweilige elektronische Verständigungsadresse und anschließender Eingabe desselben in einem Webformular durch den Empfänger)

Optional sollte der Empfänger die Möglichkeit zur Angabe von weiteren elektronischen Verständigungsadressen und einer postalische Verständigungsadresse haben. Unvalidierte Verständigungsadressen sind dabei auszuscheiden.

2.3.3.6 Schritt 4: Angabe eines Verschlüsselungszertifikats

Der Empfänger hat das Recht bzw. die Möglichkeit elektronisch zugestellte Dokumente in einer vertraulichen, d.h. in einer ausschließlich für den Empfänger lesbaren Form zu erhalten (bei manchen Verfahrensbereichen zwingend vorgeschrieben. z.B. Gesundheitsdaten). Der Empfänger kann zu diesem Zweck seinen öffentlichen Schlüssel in Form eines Verschlüsselungszertifikats angeben (siehe dazu [ZUSESPEC]). Damit kann ein Absender den öffentlichen Schlüssel dieses Zertifikats zur Verschlüsselung von Dokumenten benützen; die Vertraulichkeit ist damit gewahrt. Hinterlegt der Empfänger keinen öffentlichen Schlüssel, können sensible Daten (z.B. Gesundheitsdaten – relevante Zustellstücke) nicht elektronisch zugestellt werden. Eine diesbezügliche Information sollte bei den Anmeldeinformationen des jew. Zustelldienstes angebracht werden.

2.3.3.7 Schritt 5: Kontrolle der Daten und Zustimmung zur elektronischen Zustellung

In diesem Schritt werden die empfängerspezifischen Daten und die validierten Verständigungsadressen angezeigt. In Folge wird der Empfänger zur Bestätigung der Korrektheit dieser Daten und zur Zustimmung zur elektronischen Zustellung mittels Signatur des „Vertragstextes“ aufgefordert.

2.3.3.8 Juristische Personen

Für die Registrierung von juristischen Personen sind die Prozessschritte der natürlichen Person wie folgend abzuändern und zu ergänzen:

2.3.3.9 Schritt 1: Qualitätsvolle Identifikation

Eine für die juristische Person zeichnungsberechtigte bzw. zur Approbation für die Behörde berechtigte natürliche Person identifiziert sich analog wie im Schritt 1 bei natürlichen Personen, wobei jedoch die natürliche Person im Besitz einer elektronischen Vollmacht sein MUSS, die diese als berechtigten Zeichnungsberechtigten bzw. eine zur Approbation für eine Behörde berechtigte Person ausweist. Die Vorlage der elektronischen Vollmacht erfolgt im Zuge des Identifikationsprozesses nach dem Konzept Bürgerkarte.

2.3.3.10 Schritt 2: Ergänzung der zugehörigen Adressdaten

Nach Schritt 1 sind all jene Daten, die für eine Registrierung der juristischen Person erforderlich jedoch nicht aufgrund der Vorlage der elektronischen Vollmacht aus Schritt 1 bekannt sind zu ergänzen. Vor allem sind die Adressdaten anzugeben.

Falls möglich kann zur Beschaffung der Adressdaten auf ein zusätzliche Register zurückgegriffen werden, zum Beispiel dem Unternehmensregister . Die Identifikation der juristischen Person dort MUSS anhand der in der elektronischen Vollmacht (aus Schritt 1) enthaltenen Reigsternummer (z.B. Firmenbuchnummer, Vereinsregisternummer, etc.) eindeutig möglich sein. Andernfalls ist der Bezug von Daten aus einem Register nicht möglich.

2.3.3.11 Schritt 3 bis 5:

Bei der juristischen Person sind diese Schritte gleich denen der natürlichen Person.

2.3.4 Prozess: Absenden von Zustellstücken

Die folgenden Schritte beschreiben das Absenden eines Zustelldokuments durch eine Applikation des Absenders.

2.3.4.1 Absenden an natürliche Personen

Der Prozess Absenden von Zustellstücken gliedert sich in folgende Schritte:

2.3.4.2 Schritt 1: Abfrage des Verzeichnisdienstes Zustellung

Der Zustellkopf [ZUSEKOPF] dient neben der Bestimmung der Zustelldienstes, bei denen sich der Empfänger registriert hat, auch der Bestimmung von zugehörigen Verschlüsselungszertifikaten, zur Bestimmung von Abwesenheiten (z.B. Urlaubszeiten – siehe auch Punkt 8 in diesem Dokument), zur Bestimmung von priorisierten, zulässigen Dokumentenformaten, um zielgerichtete Zustellungen durchzuführen (z.B. Übermittlung an Architekten im Format CAD durchaus möglich) sowie des Zustelltokens für die direkte Adressierung der Sendung, welche im Zustelldienst eingegeben werden bzw. vorhanden sind.

Es gibt mehrere Möglichkeiten zur Abfrage des Zustellkopfes [ZUSEKOPF]

1. **mit vZbPK:** Sofern der Absender eine Behörde ist und das verschlüsselte Zustell-bPK des Empfängers bekannt ist, soll dieses zur Abfrage verwendet werden.

2. **mit Namen, optionaler postalischer Verständigungs-Adresse (ADR) und GEBDAT:** wird eine Zustellung in der Qualität RSa/RSb durchgeführt, so muss neben Vor-, Nachname auch das Geburtsdatum (GEBDAT) des Empfängers angegeben werden.

3. **mit Namen und Verständigungsadresse**: ist dem Absender eine elektronische bzw. postalische Verständigungsadresse des Empfängers bekannt (im Sinne der elektronischen Zustellung), so kann diese zur Abfrage und Identifikation verwendet werden.

Das Resultat beinhaltet eine Liste von Zustelldiensten, die eine elektronische Zustellung an den Empfänger erlauben.

Hinweis: Das Resultat kann mehrdeutig sein, a) weil ein Empfänger bei mehreren Zustelldiensten registriert sein kann bzw. b) aufgrund von Namens- und Adressgleichheit zu einer Abfrage mehrdeutige Treffer existieren können – siehe [ZUSELDAP]. Im Fall a) würde der Zustelldienst gewählt werden, welcher die Verschlüsselung mittels Zertifikat erlauben würde bzw. bei „gleichwertigen" Registrierungsdaten das Los entscheiden bzw. im Fall b) ist auf die konventionelle (postalische) Zustellung zurück zu greifen. Die Definition des Ergebnis-Sets ist in [ZUSELDAP][ZUSESPEC] zu finden.

Die Antwort des Verzeichnisdienstes enthält die Bestätigung der Möglichkeit der elektronischen Zustellung und außerdem zu jedem Eintrag eines Zustelldienstes ein Zustelltoken, ein Verschlüsselungszertifikat bzw. zulässige Dokumentenformate (jeweils falls vorhanden). Falls der Benutzer sich bei seinem Zustelldienst als abwesend gemeldet hat (siehe dazu auch Prozeß 7 dieses Dokuments) kommt keine Antwort bei der Abfrage retour; falls der Benutzer bei mehreren Zustelldiensten registriert ist und sich nicht bei allen Zustelldiensten als abwesend angezeigt hat, kommt dennoch eine eventuelle elektronische Zustellmöglichkeit/-dienst retour.

2.3.4.3 Schritt 2: Auswahl eines Zustelldienstes

Der Absender sucht aus der Anzahl der zurückgelieferten Zustelldienste einen Zustelldienst aus. Ein Zustelldienst, bei dem der Empfänger als abwesend gemeldet ist, darf nicht ausgewählt werden und wird deshalb auch nicht rückgemittelt – siehe auch Prozess: Temporäre Abwesenheit.

Bietet ein Zustelldienst die Möglichkeit einer verschlüsselten Übermittlung des Zustellstücks zum Empfänger, so muss dieser aufgrund der Wahrung der Vertraulichkeit bei der Auswahl gegenüber anderen höher priorisiert werden. Ansonsten ist bei gleichwertigen Optionen ein Zufallsmechanismus heranzuziehen.

2.3.4.4 Schritt 2: Verschlüsselung des Zustellstücks

Sofern bei dem ausgewählten Zustelldienst ein Verschlüsselungszertifikat des Empfängers vorhanden ist, ist dieses zur Verschlüsselung des Zustellstücks zu verwenden. Zur Verschlüsselung siehe auch [ZUSEMSG]. Die Verschlüsselung erfolgt durch den Absender.

2.3.4.5 Schritt 3: Versenden des Zustellstücks

Die Datenstruktur DeliveryRequest [ZUSEMSG] stellt den Container für die Kodierung von Zustellstücken dar. In dieser Datenstruktur sind neben der Angabe des Zustellstücks auch

zusätzliche Metadaten, welche für die elektronische Zustellung notwendig sind, enthalten. Die Verwendung von DeliveryRequest erfolgt gemäß [ZUSEMSG].

Der DeliveryRequest wird in einen MIME-Container verpackt und vom Zustelldienst geprüft, daraufhin wird dem Absender eine Statusinformation (korrekter Empfang, syntaktische Fehler, etc.) in der Webservice Antwort zurückgeliefert.

2.3.4.6 Absenden an eine juristische Person

Für das Absenden von Zustellstücken an juristische Personen sind die Prozessschritte gleich wie beim Absenden von Zustellstücken an natürliche Personen. Zu beachten ist, dass die juristische Person selbst Empfänger ist und nicht eine der annahmeberechtigten (natürlichen) Personen.

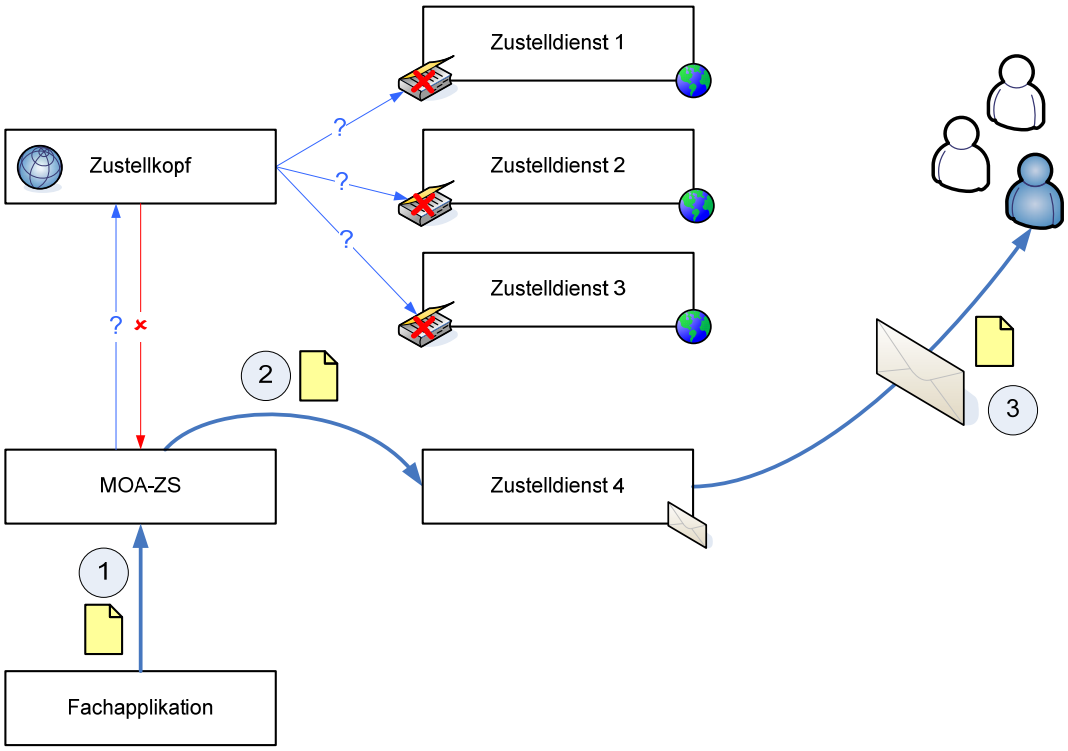
2.3.5 Prozess: Duale Zustellung

Bei der dualen Zustellung erfolgt im Falle, dass der Empfänger nicht über einen elektronischen Zustelldienst erreichbar ist, die Zustellung über einen Zustelldienst der das Zustellstück auf Papier druckt und per Briefpost an den entsprechenden Empfänger verschickt. Die Auswahl eines geeigneten Zustelldienstes für den Versand auf Papier erfolgt dabei durch die Applikation bzw. MOA-ZS unter Berücksichtigung der Möglichkeiten, wie bspw. Druck- oder Zustellformen, sowie ggf. der Zustellkosten.

2.3.5.1 Prozessmodell duale Zustellung

Wird die Middleware MOA-ZS, wie in Abbildung 3 gezeigt, zur Zustellung eingesetzt, hat die Fachapplikation nur einen einzigen Anlaufpunkt für die Zustellung und kann die Zustellung nach dem Prinzip „fire and forget“ abwickeln. MOA-ZS kann dabei die Zustellanfrage entgegen nehmen, ohne vorher die elektronische Adressierbarkeit des Empfängers zu prüfen, was wiederum die Abwicklung der Zustellung auf der Seite der Fachapplikation beschleunigt.

Abbildung 2 – Prozess der dualen Zustellung



2.3.5.2 Endverarbeitung des Zustellstücks

Die konkrete Endverarbeitung (Druck, Adressierung, Kuvertierung, etc.) eines bestimmten Dokumenttyps durch den Zustelldienst zur papierbezogenen Zustellung muss individuell vereinbart werden. Eine generische Spezifikation scheint Aufgrund der unzähligen möglichen Parameter (Papierformate und -orientierungen, Papiersorten, Druckränder, Einseiten-/Doppelseitendruck, Faltung, Kuvertierung, Adressierung, etc.), die sehr stark von den Dokumenttypen der unterschiedlichen Fachapplikationen sowie den zum Einsatz kommenden Geräten beim Zustelldienst (Druckstrasse) bestimmt sind, nicht möglich. Daher sieht die duale Zustellung die Übergabe eines Druckprofils in der Zustellanfrage vor. Dieses Druckprofil regelt die Endverarbeitung des Zustellstücks durch den Zustelldienst. Das Druckprofil kann weitere Parameter für die Endverarbeitung vorsehen, die mit der Zustellanfrage übergeben werden können. Ist die konkrete Art der Endverarbeitung für den Zustelldienst schon aus dem Typ des Zustellstücks (Dokumenttyp) ersichtlich, können Fachapplikation und Zustelldienst auch den Verzicht der Angabe eines Druckprofils vereinbaren.

2.3.5.3 Zustellung

Die Zustellung des gedruckten Zustellstücks erfolgt entsprechend den gesetzlichen Regelungen für die bestehende Papierzustellung.

Optional kann der Zustelldienst auch die Bearbeitung der Retouren übernehmen. Dazu kann er auf dem Zustellstück eine Adresse für deren Rücksendung und eine entsprechende Referenznummer vorsehen, die ihm die eindeutige Zuordnung des Zustellstücks zu einer Zustellanfrage und damit die Rückmeldung eines Fehlers, der Unzustellbarkeit oder des Zustellerfolgs an MOA-ZS bzw. die Fachapplikation ermöglicht. Selbst Papier-Retouren könnten nach einem Scan-Vorgang der elektronischen Weiterverarbeitung zugeführt werden,

entsprechendes Schema der Weiterverarbeitung ist in [ZUSEMSG] zu finden (liegt die Bestätigung bereits elektronisch vor, ist sinngemäß zu verfahren).

2.3.6 Prozess: Verständigung des Empfängers über vorliegende Zustellstücke

Eine Verständigung des Empfängers über eingegangene Zustellstück(e) kann sowohl elektronisch als auch durch eine Papierverständigung erfolgen (ähnlich der bisher von der Post verwendeten ‚Verständigung über die Hinterlegung eines Schriftstückes' – „gelber Zettel"), wobei die Reihenfolge folgendermaßen laut Zustellgesetz [ZUSTG] festgelegt ist:

1. erste elektronische Verständigung,
   a) unverzüglich vom Zustelldienst zu versenden
2. zweite elektronische Verständigung,
   a) bei nicht erfolgter Abholung innerhalb von 48 Stunden oder
   b) bei technischen Problemen der Übermittlung der ersten elektronischen Verständigung
3. dritte Papierverständigung (nicht bei Zustellungen ohne Zustellnachweis4),
   a) bei nicht erfolgter Abholung innerhalb weiterer 24 Stunden, sofern der Empfänger eine Abgabestelle (Postadresse) dem Zustelldienst bekannt gegeben hat.

Unabhängig davon, ob eine Verständigung elektronisch oder konventionell erfolgt, muss sie jedenfalls folgende Informationen enthalten:

1. das Datum der Versendung,
2. die Internetadresse, unter der das zuzustellende Dokument zur Abholung bereitliegt (URL),
3. das Ende der Abholfrist,
4. einen Hinweis auf das Erfordernis einer Signierung bei der Abholung und
5. einen Hinweis auf den Zeitpunkt, mit dem die Zustellung wirksam wird.

Ein zur Abholung bereitgehaltenes Dokument gilt spätestens mit seiner Abholung als zugestellt.[5]

Wird ein Zustellstück nicht abgeholt, ist der Zeitpunkt der Versendung der zweiten elektronischen Verständigung oder der Versendung der konventionellen Papierverständigung, sofern eine Postadresse bekannt gegeben wurde, für den Eintritt der Zustellwirkungen maßgeblich. Im ersten Fall gilt die Zustellung grundsätzlich am ersten Werktag nach der zweiten elektronischen Verständigung als bewirkt.[6] Im zweiten Fall gilt die

[4] § 36 [ZustG07]

[5] § 35 (5) [ZustG07]

[6] § 35 (6) [ZustG07]

Zustellung grundsätzlich am dritten Werktag nach der dritten postalischen Verständigung als bewirkt.[7]

In der elektronischen Verständigung sind die gleichen Inhalte mitzuteilen wie in der Papierverständigung. Die elektronische Verständigung zeigt an, ob es sich um die erste oder um die zweite Verständigung handelt. Erfolgt die elektronische Verständigung per SMS, so können die Inhalte abgekürzt werden, um mit einer SMS das Auslangen zu finden. Die SMS hat aber jedenfalls die Daten/Informationen laut § 35 (1) [ZUSTG] zu enthalten.

Die erste elektronische Verständigung ist wie in Formular 7 der Zustellformularverordnung [ZUSTFORM] vorgegeben zu gestalten.

Die zweite elektronische Verständigung ist wie in Formular 8 der Zustellformularverordnung [ZUSTFORM] vorgegeben zu gestalten.

Die Papierverständigung ist nach der Musterkarte (Postkartenformat) und rückführbar elektronisch signiert auszuprägen. Die signierten Inhalte der Mailverständigung und der Druckverständigung sind fast identisch strukturiert. Die Hinweise sind nicht signiert und sind in der E-Mail und im Druck unterschiedlich.
Die Papierverständigung ist ein 160 Gramm blassgelbe Kartonkarte. Diese wird einseitig bedruckt.

Die dritte Papierverständigung ist wie in Formular 9 der Zustellformularverordnung [ZUSTFORM] vorgegeben zu gestalten.

Diese Papierverständigung ist auf einem hinreichend starken Papier zu drucken, so dass ein getrenntes Kuvertieren nicht notwendig wird. Allenfalls ist das Layout noch anzupassen, damit die postalische Zustellung auch effizient möglich wird. Der Druckoutput wird zu vorgegebenen Zeitpunkten (z.B. 1x pro Tag) erzeugt.

2.3.6.1 Schritt 1: Verständigung der Empfänger

Nach der Annahme des Zustellstücks durch den Zustelldienst wird der Empfänger über die von ihm angegebenen elektronischen Verständigungsadresse(n) verständigt. Der Empfänger kann zusätzlich auch elektronische Verständigungsadressen seiner bevollmächtigten Vertreter bekannt geben, die dann ebenso benachrichtigt werden. Der Zustelldienst muss die erste elektronische Verständigung unmittelbar verrichten – siehe auch [ZUSTG].

2.3.6.2 Schritt 2: Erneute Verständigung

Eine erneute elektronische Verständigung erfolgt im Falle der Nichtabholung gemäß der Definitionen im [ZUSTG].

2.3.6.3 Schritt 3: Zusendung einer Papierverständigung

Wird das Zustellstück, trotz der Verständigung(en) im vorigen Schritt, innerhalb der aus dem Zustellgesetz resultierenden Frist nicht abgeholt, so erfolgt – wenn eine Postadresse angegeben wurde – eine Zusendung einer Papierverständigung an die angegebene postalische Verständigungsadresse des Empfängers. Damit ist die Verständigung z.B. auch bei technischem Gebrechen gewährleistet.

[7] § 35 (7) [ZustG07]

2.3.7 Prozess: Abholen von Zustellstücken

2.3.7.1 Schritt 1: Qualitätsvolle Identifikation

Jeder Zugriff auf geschützte Daten des Zustelldienstes darf nur nach einer qualitätsvollen Identifikation erfolgen, z.B. unter Verwendung von MOA-ID [MOA]. Auch beim Zugriff auf die URL des Zustelldienstes, welche bei der Verständigung angegeben wird, erfolgt eine solche Identifikation des Annahmeberechtigten (Identifikation: wurde im Prozess Registrierung beschrieben) laut beiliegendem Muster:

Abbildung 3 – Signatur der Anmeldedaten

Anmeldedaten:

Durch die elektronische Signatur bestätige ich, dass die bis 01.02.2012 um 10:53:33 eingelangten Zustellstücke in meinem Verfügungsbereich gelangt sind.

Daten zur Person

Name: Max Mustermann
Geburtsdatum: 15.01.1980

Daten zur Anwendung

Name: Musterzustelldienst
Staat: Österreich

Technische Parameter

URL:	https://www.musterzustelldienst.at/
Bereich:	ZU (Zustellung)
Vollmachten-Referenz:	2564613162533378374
Identifikator:	arTawjUyACUFovs9kYw/32IIU+8=
Datum:	01.02.2012
Uhrzeit:	10:53:33

Nach erfolgreicher Identifikation und Bestätigung des Erhalts einer Zustellung mit Zustellnachweis erfolgt die Offenlegung der Zustellstücke.

Anm.: § 35 Abs. 3 ZustG07 ermöglicht auch eine Identifikation und Authentifizierung durch eine an die Verwendung sicherer Technik gebundene automatisiert ausgelöste elektronische Signatur. Das heißt nach erfolgtem organisatorischen Austausch eines Zertifikates welches den Zugriff auf das Zustellpostfach des Empfängers ermöglicht werden die Schritte 2 und 3 mittels Standard-Software Produkte (E-Mail Programm, etc.) durchgeführt. Die Bestätigung der Abholung ist in dieser gewählten Variante allenfalls lt. Schritt 4 zu berücksichtigen (Details dazu siehe [ZUSEMAIL]).

2.3.7.2 Schritt 2: Auflistung der zur Abholung bereiten Zustellstücke

Eine Auflistung der abholbereiten Zustellstücke inklusive der für den Empfänger relevanten Daten (Absender, Fristen) wird dargestellt.

Hat die absendende Behörde die Empfangnahme durch eine bevollmächtigte Person ausgeschlossen, so darf einer bevollmächtigten Person (die mit der Identität des Empfängers auftritt) die bereitgehaltenen Zustellstücke nicht angezeigt werden. Eine Abholung kann nur durch den tatsächlichen Empfänger erfolgen.

2.3.7.3 Schritt 3: Download und Weiterleitung

Sowohl die Möglichkeit zum Download bzw. als auch die der Weiterleitung des Zustellstücks an eine E-Mailadresse muss dem Benutzer zur Verfügung gestellt werden. Falls das Dokument bereits vom Absender verschlüsselt wurde, so erfolgt die Weiterleitung des Zustellstücks in der Form einer E-Mail mit dem Inhalt des verschlüsselten Zustellstücks sowie eines Begleittextes. Das zu verwendende Datenformat ist in [ZUSEMSG] beschrieben.

Elektronische RSa-Schriftstücke müssen auch nach der 1. Abholung aus Sicherheitsgründen (z.B. Fehlschlag des Downloads, etc.) noch für eine Zeitspanne von 14 Tagen (siehe ZustG07) am Server abholbar gehalten werden. Der Empfänger kann die Abholung des Zustellstücks in dieser Zeitspanne wiederholen.

2.3.7.4 Schritt 4: Rückmeldung an den Absender

Erfordert die Schriftstückklasse das Ausstellen eines Zustellnachweises (siehe auch DeliveryNotification in [ZUSEMSG] und wurde das Schriftstück in Schritt 3 angenommen, so wird ein Zustellnachweis vom Zustelldienst erstellt und versendet. Bei zustellnachweispflichtigen Sendungen erfolgt das Ausstellen des Zustellnachweises unmittelbar nach der Identifikation in Schritt 1. Aus dem Text des Zustellnachweises muss der Umstand einer Abholung auf Basis §35 (3) [ZUSTG] erkennbar sein.

Der Zustellnachweis an den Absender des Zustellstücks wird in der Form einer DeliveryNotification [ZUSEMSG] erzeugt. Als Empfängeradresse des Zustellnachweises wird die „NotificationAddress“ des DeliveryRequest Containers verwendet. Diese sieht als Möglichkeit zur Übermittlung des Zustellnachweises

- an ein Webservice URL zur automatischen Weiterverarbeitung oder
- Übermittlung per E-Mail

Der Zustelldienst kann mit dem Empfänger vereinbaren, dass bereits abgeholte Dokumente nach Ablauf der Abholfrist länger als zwei Wochen bereitgehalten werden.

2.3.8 Prozess: Nichtabholung von Zustellstücken

Wird ein Zustellstück innerhalb der Frist nicht abgeholt, so ist eine elektronische Unzustellbarkeitsanzeige, in der die Nichtabholung beim elektronischen Zustelldienst vermerkt ist, sowie die entsprechenden Verständigungs-Metadaten an den Absender zu senden. Die zu verwendenden Adressierungen sind mit denen des Schritts 4 im Prozess Abholung von Zustellstücken ident.

Das Zustellstück ist im Falle der Nichtabholung nach Ablauf der zweiwöchigen Frist zu löschen[8].

2.3.9 Prozess: Temporäre Abwesenheit

Ein Annahmeberechtigter kann in Zeiten, in denen für ihn eine Abholung von elektronischen Zustellungen nicht möglich ist, eine Abwesenheitsschaltung bei seinem Zustelldienst aktivieren. Der Zeitraum in welchem die Abwesenheitsschaltung aktiv ist, wird auch im Verzeichnisdienst [ZUSELDAP] des Zustelldienstes bzw. Zustellkopfs [ZUSEKOPF] geführt. Während dieser Zeit kann keine elektronische Zustellung (im Sinne des ZustG07) erfolgen.

[8] § 35 (4) [ZustG07]

2.3.10 Prozess: Abmeldung vom Zustelldienst

Sollte ein Empfänger die Services eines elektronischen Zustelldienstes nicht mehr nutzen wollen, so muss dem Empfänger eine einfache Möglichkeit zur Abmeldung vom Zustelldienst bereitgestellt werden. Die Abmeldung von einem Zustelldienst kann unter Verwendung der Bürgerkarte oder durch eine vom Empfänger unterschriebene schriftliche Erklärung erfolgen. Sie wird mit ihrem Einlangen beim Zustelldienst wirksam.

2.3.11 Prozess: Administration

Eine Veränderung der im Prozess **„Registrierung“** angegeben Daten, die ein Empfänger oder ein Annahmeberechtigter eingeben darf, muss auch nachträglich möglich sein. Vor jeder Veränderung dieser Daten muss eine qualitätsvolle Identifikation erfolgen.

2.4 Protokollierung

Eine Protokollierung der Aktionen der Empfänger ist in geeigneter Weise vorzusehen – das genaue Prozedere wird in den technischen Rahmenbedingungen zum Betrieb des jew. elektronischen Zustelldienstes festgelegt (bzw. siehe [ZUSESPEC] und [ZUSEMSG]). Die Dauer der Archivierung und der enthaltene minimale Umfang der Protokollierung ist den genannten Spezifikation bzw. gesetzlichen Rahmenbedingungen[9] der Zustellung zu entnehmen.

2.5 Zusätzliche Funktionen

Die Implementierung von zusätzlichen Funktionen welche die Sicherheit des Systems Zustellung erhalten und nicht weiter einschränken bzw. für den Benutzer einen Mehrwert darstellen ist dem Betreiber freigestellt, z.B. ein Dokumentensafe (in welchem Empfänger die bereits zugestellten Zustellstücke längerfristig aufbewahren können), der Ausdruck der zugestellten Dokumente[10], die Speicherung auf gängigen Speichermedien, etc.

2.5.3 Notifikation für neu eingelangte Zustellungsstücke während einer offenen Session

Wenn während einer offenen Session neue Zustellstücke einlangen, muss der Empfänger auch (mittels Notifikation) darüber informiert werden. Die neuen Zustellungsstücke können erst bei der nächsten Anmeldung angezeigt werden. Keinesfalls dürfen neu eingelangte Zustellungsstücke sofort in einer offenen Session des Benutzers angezeigt werden. Das gilt auch für die Abholung auf Basis einer besonderen Vereinbarung (gem. §35(3) [ZUSTG]).

2.5.4 Eintragung Private Zusendung ja/nein

Der Benutzer kann bei der Registrierung bestätigen, ob er auch private Zusendungen[11] erhalten möchte (Details dazu siehe [ZUSESPEC]).

[9] § 29 (1) Z 7 [ZustG07]

[10] § 29 (1) Z 10 [ZustG07]

[11] § 29 (3) [ZustG07]

2.5.5 Kostenersatz

Die Verrechnungsleistung[12] der anfallenden Zustellkosten wird organisatorisch vom Zustelldienst, welcher auch den Zustellkopf inne hat durchgeführt (Details dazu siehe [ZUSERECH].

2.5.6 Löschen eingelangter Zustellungsstücke

Zustellstücke dürfen nach Anmeldung beim Zustelldienst (Systemeinstieg) vom Empfänger nicht gelöscht werden können bevor ihm diese angezeigt wurden. Nach 14 Tagen sind Sie allerdings auf Grund der gesetzlichen Vorgaben[13] zu entfernen.

2.5.7 Authentifizierung von Sendern

Der Sender authentifiziert sich nach erfolgter Registrierung beim Zustelldienst (siehe dazu auch [ZUSEMSG] mittels Client-Zertifikats mit Verwaltungs- oder Dienstleistereigenschaft.

[12] § 29 (2) [ZustG07]

[13] § 35 (4) [ZustG07]

3 Schnittstellen

Das Modell enthält drei Schnittstellen: **Empfänger – Zustelldienst**, **Behörde (Sender) – Zustelldienst** und die **Verständigung**. Wie bereits erwähnt, kann sich die Verständigung unterschiedlichster, in der Praxis erprobter Medien bedienen und wird deshalb nicht näher beschrieben.

3.1 Empfänger – Zustelldienst

Im Rahmen des österreichischen E-Government Konzeptes werden an die Empfänger nur folgende Anforderungen gestellt: ein webfähiger Computer und die Möglichkeit der Erstellung elektronischer Signaturen. Daraus ergeben sich implizit die Rahmenbedingungen für die Schnittstelle:

- Die Benutzerführung und Kommunikation finden über Webseiten statt.
- Die Signatur erfolgt über die Security-Layer Schnittstelle [HOKP01] des österreichischen Bürgerkartenkonzepts.

Nachdem sich also der Empfänger gegenüber dem Zustelldienst mittels Signatur authentifiziert hat[14], bekommt er eine Liste aller zuzustellenden Schriftstücke angezeigt. Implizit wird aus der bestehenden Session mit dem Empfänger heraus ein vom Zustelldienst signierter Zustellnachweis vom Zustelldienst an den Sender für zu bestätigende Zustellstücke rückübermittelt. Daraufhin werden die Dokumente zum Herunterladen frei geschaltet. Freigeschaltete Dokumente können entweder unmittelbar oder zu einem späteren Zeitpunkt (auch mehrfach) herunter geladen und entschlüsselt werden.

Zum Benutzer ist eine https:// Verbindung vorzusehen, es dürfen nur Verbindungen mit starker SSL Verschlüsselung gemäß dem Stand der Technik aufgebaut werden.

3.2 Behörde (Sender)– Zustelldienst

Die Schnittstelle zwischen Behörde (Sender) und Zustelldienst ist eine zweistufige Schnittstelle. Zur Auswahl des Zustelldienstes und Abfrage relevanter Metadaten kommt ein Verzeichnisdienst mit LDAP-Schnittstelle via Anfrage an den Zustellkopf zum Einsatz. Zur Übermittlung des Schriftstücks wird ein Webservice (XML und SOAP) benützt. Die Funktionen die über diese Schnittstellen abgewickelt werden, sind im Einzelnen:

- Das Abfragen eines Zustelldienstes via Zustellkopf (inklusive Verschlüsselungsschlüssel, zulässiges Dokumentenformat, etc.) zu einer bestimmten Person
- Das Übersenden (Hinterlegen) eines Schriftstückes für eine Person
- Das Übermitteln eines Zustellnachweises
- Das Durchführen einer Rückzustellung (bzw. Übermittlung einer entsprechenden negativen Nachricht), sprich Unzustellbarkeitsanzeige.

[14] Die in diesem Schritt stattfindende Authentifizierung des Empfängers setzt die Bürgerkarte oder eine auf Grund einer besonderen Vereinbarung des Empfängers mit dem Zustelldienst an die Verwendung sicherer Technik gebundene automatisiert ausgelöste Signatur voraus.

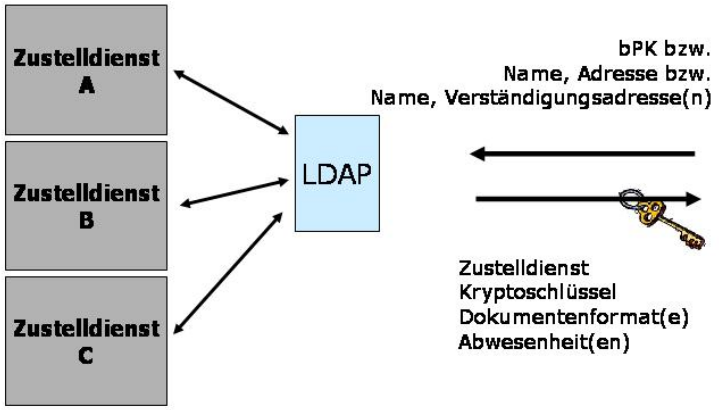
Eine genauere Beschreibung der einzelnen Funktionalitäten und Prozesse entnehmen Sie bitte dem Abschnitt 2.3 dieses Dokumentes.

Die im Folgenden beschriebenen Funktionalitäten (Abfrage des Zustellkopfes, Stammzahlenregisterabfrage zwecks bPK Berechnung für die Zustellung, Verschlüsselung, Signatur) können auch durch das Modul MOA-ZS[15] abgearbeitet werden.

3.2.3 Ermittlung des Zustelldienstes

Um den für den Empfänger relevanten Zustelldienst zu erfragen bzw. eine Verschlüsselung des Dokumentes durchführen zu können, führt der Sender eine Abfrage beim zentral eingerichteten Zustellkopf, einem Service, durch (siehe auch [ZUSEKOPF]).

Abbildung 4 – Ermittlung des Zustelldienstes



Im ersten Schritt sendet die Behörde (Sender) die Daten des Empfängers an den Verzeichnisdienst. Diese Daten müssen ausreichen, um die Person eindeutig zu identifizieren; Name und Adresse des Empfängers müssen in ZMR-konformer Schreibweise vorliegen – eine „unscharfe“ Suche ist für Adressen nicht nicht vorgesehen (z.B. Wildcards). Eine Bulk-Abfrage zur Vereinfachung des technischen Ablaufs ist jedoch vorgesehen. Drei mögliche Varianten werden derzeit realisiert:

- Identifikation basierend auf der Zahl des Stammzahlenregisters (SZR). Aus Datenschutzgründen wird aber nicht die Stammzahl selbst, sondern eine verschlüsselte Einwegableitung daraus verwendet [HOLL02] – ein dem Verzeichnisdienst vorgeschalteter Proxy übernimmt die Entschlüsselung der angelieferten verschlüsselten bPKs zur Durchführung der Abfrage; Bildung der bPK siehe auch Abschnitt 3.2.2.
- Identifikation basierend auf Name, Geburtsdatum und optional elektronische oder postalische Verständigungsadresse.

[15] http://egovlabs.gv.at/projects/moa-zs/

Ist der Empfänger dem Verzeichnisdienst bekannt, so übermittelt dieser im zweiten Schritt den oder die zuständigen Zustelldienste sowie die empfängerspezifischen, öffentlichen Schlüssel zur Verschlüsselung – diese Daten stammen aus der jeweiligen Benutzer-Information beim Zustelldienst. Die Gründe, den Verschlüsselungsschlüssel nicht gleich beim Antrag (d.h. beim Start des Verfahrens) zu erfragen, ergibt sich dadurch, dass es Verfahren gibt, die ursprünglich nicht von Seiten des Empfängers angestoßen werden, zum Beispiel Strafverfügungen. Diese Verfahren wären ansonsten von einer elektronischen Zustellung ausgeschlossen.

Mögliche Adresskonflikte, welche durch die Angabe einer Wunsch-Zustelladresse während des Verfahrens, als Ergebnis der Anfrage beim Verzeichnisdienst der Zustelldienste (bei mehreren Möglichkeiten obliegt die Wahl des Zustelldienstes allein dem Absender), als Ergebnis einer ZMR-Abfrage (Hauptwohnsitz, etc.) bzw. bei nicht Vorhandensein der bereits aufgezählten Adressmöglichkeiten, durch die Heranziehung einer (möglicherweise vorhandenen) „Absenderadresse“ entstehen, sollen in der folgenden Reihenfolge aufgelöst werden (d.h. bei Vorhandensein einer höher priorisierten Adresse, muss diese verwendet werden):

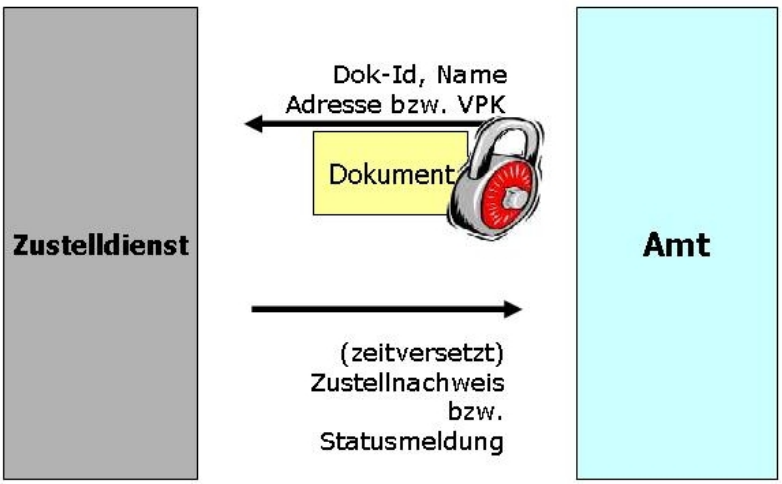
- bei Verzeichnisdienst erfragte Zustelldienst Adresse(n)
- im Verfahren genannte Zustelladresse, Absendeadresse
- eruierte (ZMR-)Hauptwohnsitzadresse

Im Folgenden soll nur die Hinterlegung näher beschrieben werden, da das Übermitteln des Zustellnachweises bzw. die Durchführung einer Rückzustellung/Unzustellbarkeitsanzeige über die Schnittstelle Behörde – Zustelldienst nur einfache Request-Response Abwicklungen sind.

3.2.4 Hinterlegung eines Schriftstückes

Das Protokoll zur Hinterlegung eines Schriftstückes sieht das Übermitteln des verschlüsselten Dokumentes an den im vorigen Schritt gewählten Zustelldienst vor (siehe auch [ZUSEMSG]. Das folgende Bild verdeutlicht den Ablauf:

Abbildung 5 – Hinterlegung eines Schriftstückes



Die Behörde (Sender) signiert und verschlüsselt das Dokument und übergibt es an den Zustelldienst (inkl. möglicher Zustellnachweiserfordernisse, etc.) – Details zur Verschlüsselung und dem Nachrichtenformat siehe [ZUSEMSG]. Die Reihenfolge (zuerst

signieren, dann verschlüsseln) ist bedingt durch den Umstand, dass zugestellte Schriftstücke in Klartextform mit intakter Signatur weitergegeben können werden sollen.

Der Problematik bei der Identifikation des gewünschten Empfängers kann durch die Verwendung der bPK begegnet werden. Namen, Wohnadressen, Verständigungsadressen können sich im Laufe der Zeit ändern. Es wird deshalb allgemein empfohlen, elektronische Zustellungen unter der Verwendung der bPK vorzunehmen. Diese bPK (für den Verfahrensbereich Zustellung) wird mittels des vorgelagerten Moduls/Services als SZR-Anfrage vom Sender realisiert [SZR-SPEC]. Nach der Übermittlung von Name, Vorname und (Quell-)bPK der zustellenden Applikation (sowie optional der Adresse und des Geburtsdatums) und des Ziel-Geschäftsbereiches (in diesem Fall: ZUSTELLUNG) errechnet das SZR-Service unter Zuhilfenahme der vorliegenden Daten die verschlüsselte Zustell-bPK und liefert sie an die anfragende Behörde retour:

- (Schritt 1: Name, Vorname, Geburtsdatum für Suche im ZMR und Berechnung „Quell“-bPK(=zustellende Applikation)
- Schritt 2: bei nicht vorhandener Eindeutigkeit wird mitgelieferte „Quell“-bPK mit errechneten bPKs aus Schritt 1 verglichen;
- Schritt 3: Berechnung der „Ziel“-bPK für die im Schritt 2 ausgewählte Person

Die rückgelieferte Zustell-bPK dient forthin als Identifikations-Token zur Einsortierung beim elektronischen Postfach des Empfängers.

3.2.5 Übermitteln des Zustellnachweises

Besteht die Anforderung seitens des Senders einer Rückübermittlung eines Zustellnachweises bzw. ebenso einer möglichen Unzustellbarkeit, so werden diese an den Absender entweder an ein Webservice des Absenders oder an eine E-Mailadresse übermittelt; E-Mail stellt dabei eher den kleinsten gemeinsamen Nenner dar. Die Nachweise enthalten die zustellungsrelevanten Meta-Daten hinsichtlich Zeitpunkt der Abholung, Identifikationsmerkmale der Sendung, etc.

Tatsächlich gibt es Protokolle, die eine bessere Abwicklung eines Dokumententausches (Schriftstück gegen Zustellnachweis) gewährleisten [ASOK98], [ASSW97], [PEPS01], [GAPV99], [SHMI00]. Folgende Gründe sprechen aber für die gewählte pragmatische und einfache Lösung:

- Die Protokolle benötigen einen vertrauenswürdigen Dritten. Die amtliche Zustellung kann aber (von Gesetzes wegen) nicht von der Aussage einer außerbehördlichen Institution abhängen.
- Unter Ausschluss eines Dritten kann kein Protokoll gewährleisten, dass Sender (Behörde bzw. Zustelldienst) und Empfänger gleichzeitig(!) in Besitz der gewünschten Information kommen (Schriftstück bzw. Zustellnachweis) [PAGA99]. Bricht die Kommunikation zu einem bestimmten Zeitpunkt ab, ist der Empfänger in Besitz des (lesbaren d.h. entschlüsselbaren) Schriftstücks und der Sender nicht in Besitz des Zustellnachweises oder umgekehrt.
- Auch eine Signatur des Empfängers über das verschlüsselte Dokument könnte als Zustellnachweis benützt werden. Dies bedingt jedoch, dass die Behörde das ursprüngliche Dokument (inklusive Schlüssel der zur Verschlüsselung benützt wurde) evident hält, um jederzeit die Signatur nachprüfen zu können.

Die zur Anwendung kommende Lösung geht im zweiten Punkt zu Lasten des Empfängers. D.h. bricht die Kommunikation zu einem beliebigen Zeitpunkt ab, ist der Sender zwar in Besitz des Zustellnachweises, der Empfänger aber noch nicht in Besitz des Schriftstücks.

Das Problem wird insofern relativiert, als der Zustelldienst die Schriftstücke auch nach (scheinbar) erfolgreicher Abwicklung noch einige Zeit speichert (einige Tage bis Wochen bzw. generell parametrisierbar) und Zugriff ohne erneute Ausstellung eines Zustellnachweises erlaubt (Nachweis muss nur einmal erbracht werden). Sollte es sich nicht um ein temporäres Problem handeln (z.B. Defekt des Computers des Empfängers), weiß der Empfänger aber um das Schriftstück und kann entsprechend tätig werden (Benachrichtigung der Behörde über die technische Unmöglichkeit der Abholung und Ersuchen um eine neuerliche Zustellung - gilt als Einspruch).

Die im dritten Punkt angesprochene Möglichkeit wird nicht benutzt, da die Evidenthaltung der ursprünglichen Dokumente derzeit seitens der Behörden nicht erwünscht bzw. nicht möglich ist. Meist kann zwar der Inhalt aus den Datenbeständen rekonstruiert werden, nicht aber in einer Bit für Bit identischen Form, wie das für eine Signaturprüfung notwendig ist.

Die gewählte Vorgangsweise ist eine pragmatische und passt sich den Rahmenbedingungen an. Sie bietet im Regelfall genügend Sicherheit (durch Wiederholbarkeit des Vorganges), dass Ausnahmesituationen, wie eine notwendige Verständigung der Behörden seitens des Empfängers über „technische Probleme“ in der Praxis wohl selten auftreten sollten.

3.2.6 Daten des Zustellnachweises

Der Zustellnachweis (bzw. die Unzustellbarkeitsanzeige) enthält nur Metadaten über das zuzustellende Dokument, um sie beim Absender wieder einordnen zu können, jedoch keine Prüfsummen (Hash-Werte) über inhaltlichen Daten des Dokuments. Dies deshalb, um eine im vorigen Punkt beschriebenen Evidenthaltung der Schriftstücke auf Senderseite nicht nötig zu machen.

Aber auch aus Gründen der Geheimhaltung (gegenüber Dritten bzw. dem Zustelldienst) befinden sich keine Hinweise auf den Dokumentinhalt im Zustellnachweis.

Die Daten des Zustellnachweises reduzieren sich also auf:

- Angaben zum Absender: Name und Anschrift des Absenders
- Angaben zum Empfänger: Name und Daten zur Identität (inklusive bPK) (siehe [ZUSEMSG])
- Eindeutige Bezeichnung des Schriftstücks: zum Beispiel durch Angabe einer nicht sprechenden Nummer.
- Angaben zum Zeitpunkt der Hinterlegung und der Abholung bzw. Verständigungszeitpunkte und Fristen bei Nichtabholung.

4 Formate

XML ist das zentrale Dokumentformat im österreichischen E-Government Konzept. XML bietet eine breite Applikationsbasis (auch Open-Source), ist gut strukturierbar, bietet Standards zur Signatur und Verschlüsselung und kann mittels Stylesheets gut dargestellt werden.

Das XML wird dabei in einer Zwiebelstruktur aufgebaut. Als äußere Hülle dient eine generische XML-Container Struktur, die Daten der eigentlichen Zustellung enthalten (siehe auch [ZUSEXSD]). Für jeden Schriftstücktypen, wie z.B. den Bescheid gibt es zunehmend speziellere Strukturen. Sinn dieser Zwiebelstruktur ist es, eine Homogenisierung von Daten zu erreichen, welche zu erwünschten Synergieeffekten führt, wie z.B. die Verwendung von generischen Applikationsmodulen.

Zudem wird Augenmerk darauf gelegt, dass diese Schriftstücke als Eingangsdaten anderer Verwaltungsprozesse dienen können. Ein opakes, unstrukturiertes Format würde einer solchen Weiterverarbeitung hinderlich sein. Eine Rekonstruktion des elektronischen Schriftstücks (inklusive einer Amtssignatur) aus einem Papierausdruck ist ebenfalls ein wichtiges Designkriterium (siehe [EGOVG07]).

Trotz der Argumente für die Verwendung von XML kann **jedes beliebige Datenformat** Gegenstand der Zustellung sein. Für die verwendeten Protokolle und Mechanismen sind die Daten selbst eine „black box“ und enthalten für die Durchführung des Zustellprozesses selbst keine notwendigen Daten. Es ist also auch möglich z.B. PDF, ZIP, etc. oder andere Dateiformate zuzustellen.

4.1 Format für verschlüsselte Daten

Bei der Verschlüsselung von Daten ergibt sich die Notwendigkeit eines generischen Containers für die Verschlüsselung. Schließlich besitzen nur die wenigsten Dateiformate eine inhärente Verschlüsselungsmöglichkeit, welche falls vorhanden noch von Format zu Format unterschiedlich ausgeprägt sind.

Andererseits soll für den Empfänger der Vorgang des Entschlüsselns so unkompliziert wie möglich sein, bevorzugt mit Mechanismen, die keine Installation zusätzlicher Entschlüsselungsprogramme erfordern.

Eine pragmatische Lösung bietet der Einsatz von den im e-Mailverkehr verwendeten Formaten RFC 2822 [RFC2822], S/MIME [SMIME] und CMS [CMS]. Dabei wird wie folgt vorgegangen:

- Der Absender verschlüsselt das Schriftstück als CMS bzw. als S/MIME.
- Der Zustelldienst bildet aus dem CMS ein S/MIME und daraus eine RFC 2822 konforme Nachricht. Der so erzeugte Verschlüsselungs-Container hat das Format einer regulären e-Mail Nachricht.
- Sowohl beim Download durch den Empfänger wie dem Versand per e-Mail kann das e-Mailprogramm des Empfängers (!) die Entschlüsselung vornehmen.

Die Vorteile dieser Variante sind, dass der Großteil der kommerziell oder frei erhältlichen e-Mail Programme S/MIME Nachrichten entschlüsseln können. Es ist also nicht notwendig zusätzliche Programme zu installieren. Auch die Metapher der e-Mail als die Daten

(Anhänge bzw. Attachments) enthaltender Container ist bekannt und geläufig, sodass keine Hemmschwelle bzw. Umlernen auf Seiten der Empfänger notwendig ist. Zudem können so sogar mehrere verschiedene Dateien simpel in einem einzigen Schriftstück zusammengefasst werden. Siehe auch [ZUSEMSG].

5 Conclusio

Das beschriebene Modell bietet Vorteile für alle Beteiligten:

Für die Behörde (den Absender) ergeben sich Synergie- und Einsparungseffekte. Nicht nur durch die elektronische Zustellung an sich (keine Papier-, Druck- und Portokosten), sondern weil der gesamte Zustellprozess von der Applikation entkoppelt werden kann. Auch dass E-Government Verfahren nun durchgängig ohne Medienbruch möglich sind und z.B. Bescheide wieder als Eingangsdaten anderer Prozesse dienen können, erlaubt E-Government in einer neuen Dimension und Qualität.

Für natürliche Personen, aber auch Organisationen und Unternehmen, da sie einfach und unkompliziert zu jedem Zeitpunkt und ortsunabhängig auch persönliche Zustellungen entgegennehmen können und sich so einen Gang auf das Postamt sparen.

Für die Betreiber der Zustelldienste, da durch das offene Konzept die Möglichkeit des Betriebs der Zustellung durch die Wirtschaft möglich ist und ein Markt mit großem Volumen entstehen kann. Zudem können die Zustelldienste auch von der Privatwirtschaft für z.B. Rechnungen und andere Schriftstücke genutzt werden. Ob dabei der Zustellnachweis in der gleichen Qualität wie bei der amtlichen Zustellung notwendig ist, hängt letztlich vom jeweiligen Anwendungsfall ab.

A. Abbildungsverzeichnis

B. Tabellenverzeichnis

C. Revision History

Version	Datum	Autor(en)	
1.0.0	6.5.2004	Peter Reichstädter (BKA) Arne Hollosi (IKT-Stabstelle)	Erstellt
1.3.0	03.03.2008	Peter Reichstädter (BKA)	Anpassung auf Grund der Novellierung ZustG07 und EgovG07 Verrechnungs-Organisation Anpassung Versionsnummer zu ZUSE-Suite 1.3.0
1.3.1	04.04.2008	Peter Reichstädter (BKA)	Anpassung auf Grund feedback der AG ZUSE
1.4.0	02.02.2012	Arne Tauber (EGIZ) PeterReichstädter (BKA)	Anpassung an ZUSE Version 1.4.0

D. Referenzen

[ASOK98]	N. Asokan, “Fairness in electronic commerce”. Ph. D. thesis, University of Waterloo, 1998
[ASSW97]	N. Asokan, Victor Shoup, and Michael Waidner, “Asynchronous protocols for optimistic fair exchange”, Research Report RZ 2976 (#93022), IBM Research, November 1997
[AVG07]	Allgemeines Verwaltungsverfahrensgesetz 1991, BGBl. Nr. 51, idF. BGBl. I Nr. 5/2008.
[CMS]	Hously, R.: RFC 2630: Cryptographic Message Syntax (CMS). IETF Request For Comment, Juni 1999. http://www.ietf.org/rfc/rfc2630.txt.
[DOKFORM]	Liehman, Martin, … / AG Internet-Policy: Dokumentenformate 1.0.2, April 2005
[EGOVG07]	Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG), BGBl. I Nr. 10/2004, idF. BGBl. I Nr. 7/2008.
[GAPV99]	F. C. Gartner, H. Pagnia, and H. Vogt, “Approaching a formal definition of fairness in electronic commerce”, in Proceedings of the International Workshop on Electronic Commerce (WELCOM'99), Lausanne, Switzerland, October 1999
[HOLL01]	Arno Hollosi: Sicherheit der Verfahrenskennung, November 2001.
[HOLL02]	Arno Hollosi: Algorithmus zur Berechnung der verfahrensspezifischen Personenkennzeichnung (bPK), Februar 2002.
[HOKP01]	Arno Hollosi, Gregor Karlinger, Reinhard Posch: Security-Layer zur Bürgerkarte, November 2001.
[MIME]	Freed, N. und Borenstein, N.: RFC 2046: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types. IETF Request For Comment, November 1996. http://www.ietf.org/rfc/rfc2046.txt.
[MOA]	Stabstelle IKT-Strategie des Bundes: Module für Online Applikationen, November 2002. http://www.egovlabs.gv.at
[PAGA99]	Henning Pagnia and Felix C. Gärtner, "On the impossibility of fair exchange without a trusted third party", Technical Report, TUD-BS-1999-02, Darmstadt, Germany, 1999

[PEPS01]	Peng Liu and Peng Ning and Sushil Jajodia, "Avoiding Loss of Fairness Owing to Process Crashes in Fair Data Exchange Protocols", Decision Support Systems, Vol. 31, No. 3, 2001, pages 337-350.
POWB02]	Reinhard Posch et al: Weißbuch Bürgerkarte, Stand Mai 2002.
[RFC2822]	P. Resnick, Editor, RFC 2822: Internet Message Format, April 2001, http://www.ietf.org/rfc/rfc2822.txt
[SHMI00]	V. Shmatikov and J. Mitchell, “Analysis of abuse-free contract signing”, in Financial Cryptography '00, Anguilla, 2000
[SIGG07]	Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), BGBl. I Nr. 190/1999 idF. BGBl. I Nr. 8/2008.
[SIGV07]	Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung - SigV), BGBl. II Nr. 3/2008.
[SMIME]	RFC: 2633 S/MIME Version 3 Message Specification. B. Ramsdell, Ed. June 1999. http://www.ietf.org/rfc/rfc2633.txt
[SZR-SPEC]	Rainer Hörbe, Anforderungen an das Stammzahlen-Register
[VOLLMACH]	Thomas Rössler, Elektronische Vollmachten – Spezifikation (elvm_spez), Version 1.0.0, Mai 2006
[ZUSTG]	Bundesgesetz vom 1. April 1982 über die Zustellung behördlicher Schriftstücke (Zustellgesetz), BGBl. Nr. 200/1982, idF. BGBl. I Nr. 5/2008.
[ZUSEXSD]	Peter Reichstädter, XML-Spezifikation der Zustellungsdaten-Struktur, März 2008
[ZUSEKOPF]	Tauber A., Rössler T., Elektronische Zustellung - Zustellkopf Schnittstellenspezifikation.
[ZUSELDAP]	A. Tauber, P. Reichstädter, Zustellverzeichnis – LDAP Schema-Beschreibung, 1.4.0
[ZUSEMAIL]	Posch R., Rössler T., Elektronische Zustellung – Abholung von Zustellung über E-mail Clients, 1.4.0
[ZUSEMSG]	Tauber A., Rössler T., Elektronische Zustellung – Message Spezifikation 1.4.0.
[ZUSEMOD]	Reichstädter P., Modell und Prozesse der elektronischen Zustellung.

[ZUSERECH]	Tauber A., Reichstädter P., Modell und Prozesse der Zustellungs-Verrechnung, 1.4.0.
[ZUSESPEC]	A. Tauber, T. Rössler, P. Reichstädter, Elektronische Zustellung – Technische Spezifikation, 1.4.0
[ZUSTFORM]	Verordnung der Bundesregierung vom 30. November 1982 über die Formulare für Zustellvorgänge (Zustellformularverordnung 1982 – ZustFormV), BGBl. Nr. 600/1982 idF BGBl. II Nr. xxx/2008.